International Journal of Social Science Research and Review

http://ijssrr.com
editor@ijssrr.com
Volume 5, Issue 11
November, 2022
Pages: 426-434

Law Enforcement Policy for Mayantara Crime (Cyber Crime) in Indonesia

Rayan Al Qabooli; Joko Setiyono

Master of Law Study Program, Faculty of Law, Diponegoro University Jl. Imam Bardjo, SH No. 1-3 Pleburan UNDIP Campus, Semarang 50241, Indonesia

Email: aqrayan@yahoo.co.id

http://dx.doi.org/10.47814/ijssrr.v5i11.785

Abstract

In the 2020 cyber police KA Bareskrim Polri confirmed that there had been a significant increase in cyber activity. This study aims to examine law enforcement as an effort to overcome cybercrime and efforts to deal with the occurrence of mayantara crime. The researcher uses a normative juridical approach that is using a positivist legal idea. This concept oversees the law as a normative system that is independent, closed and detached from the real life of society. Law enforcement in overcoming cybercrimes in Indonesia has not been implemented optimally. The factor that has the most influence on the weakness of existing law enforcement in dealing with cybercrimes in the anatomy of transnational crime is the legal factor (legal substance) which contains many weaknesses and law enforcement factors. Efforts to overcome these crimes can be in the form of preventive efforts and repressive efforts. Preventive efforts are preventive efforts made to prevent the emergence of a crime within the scope of society. Repressive efforts are one of the efforts that are conceptual in nature, where these efforts are carried out after the occurrence of a crime.

Keywords: *Policy; Law Enforcement; Mayanta Crime*

Introduction

1. Background

The current world civilization is characterized by the phenomenon of advances in information and communication technology that take place in almost all areas of human life. The revolution generated by information and communication technology is usually seen from the perspective of decreasing geographical distances, eliminating national boundaries and time zones and increasing efficiency in data collection, dissemination, analysis and possibly also use.[1]Technology that is developing very rapidly has many good and bad impacts on human life. Globalization is one of the causes of rapid and limitless technological developments. Thinking power that also develops causes the emergence of a knowledge. For this knowledge, not everyone can use it wisely and correctly, so that it is very detrimental to many

[1]Budi Kristian Bivanda Putra, "Cyber Crime Application Policy in Indonesia", Pamulang Law Review, Vol.1 Issue 1, 2018, p. 2

people.[2]For example, the crime of hacking or hacking arising from the negative impact of technological progress.

In the era of globalization, the development of information and communication technology has resulted in increasingly rapid information traffic. As a result, access to information and communication is easier for everyone to get without any time and space barriers. Globalization in the world economy, especially the world of commerce, is one of the aspects of life that has been impacted by the presence of fast and reliable communication media so that business activities in various countries tend to increase.[3]Crimes committed through technology or cyberspace are called cybercrimes.

*Cyber crime*is a form or a new dimension of crime today that has received special attention in the international world. Cybercrime is currently the impact of the transition from the industrial era with the main issue being that energy using an energy transportation system can be transferred from one place to another, to the post-industrial era (post-industrial) with the main issue being that information through the use of communication systems can be exchanged. information.[4]

In the 2020 cyber police KA Bareskrim Polri confirmed that there had been a significant increase in cyber activity. Types of crimes such as "fraud, defamation, hate speech, pornography, and distribution of problematic content", are the highest ranking list in cases of cyber crime. The pandemic situation has turned society into an information society that enables cyber crime.[5]

The government has regulations regarding crimes committed through technology, namely Law no. 19 of 2016 changes to Law no. 11 of 2008 concerning Information and Electronic Transactions (hereinafter referred to as the ITE Law). The ITE Law is an effort to enforce the law against the occurrence of criminal acts of cybercrime.

2. Theoretical framework

a. Legal Certainty Theory

Legal certainty is a guarantee regarding the law that contains justice. Norms that promote justice must really function as rules that are obeyed. According to Gustav Radbruch, justice and legal certainty are permanent parts of law. He is of the opinion that justice and legal certainty must be considered, legal certainty must be maintained for the security and order of a country. Finally positive law must always be obeyed. Based on the theory of legal certainty and the values to be achieved are the values of justice and happiness.[6]

Gustav Radbruch put forward 4 (four) fundamental things related to the meaning of legal certainty, namely:

1) First, that law is positive, meaning that positive law is legislation.
2) Second, that law is based on facts, meaning that it is based on reality.
3) Third, that facts must be formulated in a clear way so as to avoid misunderstandings in meaning, besides being easy to implement.
4) Fourth, positive law should not be easily changed.

[2] Ngafifi, "Technological Progress and Human Life Patterns in a Socio-Cultural Perspective", Journal of Educational Development: Foundations and Applications, Vol. 2 No.1, 2014, p.30
[3]Dikdik M. Arief Mansur and Elisatris Gultom, 2005, Cyber Law Legal Aspects of Information Technology, Refika Aditama, Bandung, p.123
[4]Barda Nawai Arief, 2006, Mayantara's Crime: Development of Cyber Crime Studies in Indonesia,PT.Raja Grafindo Persada, p.1
[5] JPNN, 2020. Retrieved from the Number of Cyber Crimes Has Significantly Increased in the Last Five Years: https://www.jpnn.com/news/nomor-kejahatan-siber-menin_gkat-signifikan-dalam-lima-tahun-terakhir
[6]Achmad Ali, Revealing the Law (A Philosophical and Sociological Study), Publisher Toko Gunung Agung,Jakarta,2002,p.82-83

b. Criminal Law Policy Theory

Criminal law policy is an integral part of social policy, law enforcement policy, and criminal policy, which includes rational efforts in tackling crime, to achieve national goals, namely community protection and community welfare. According to Sudarto, legal policy or legal politics is an attempt to realize good regulations in accordance with the circumstances and situation at a time and the policies of the state through authorized bodies to establish the desired regulations which are expected to be used to express what is contained. in society and to achieve what is aspired to.[7]

3. Problems

Based on this description, the writer makes the formulation of the problem for writing this article, which is as follows:

a. How is law enforcement as an effort to overcome cyber crime?
b. What are the efforts to deal with the occurrence of mayantara crime?

4. Novelty/Originality of Research Results

Research on Criminal Law Policy on Chemical Castraction Sanctions against Perpetrators of Sexual Crimes against Children is original research, researchers have compared it from previous studies that discussed chemical castration sanctions. However, this study has a different discussion substance from previous studies. The following are references to previous journals that researchers used:

a. Research by Yuwono Prianto, Nabila Annisa Fuzian, and Afif Farhan, entitled "Constraints of Law Enforcement Against Cyber Crime During the Covid-19 Pandemic", Senapenmas Journal, October 2021. This research examines the appropriateness of the implementation of Law No.11/2008 Regarding Electronic Transaction Information as a means of enforcing cybercrime law during a pandemic and obstacles to law enforcement against cybercrime during a pandemic. Cyber-crime needs to get special attention from law enforcers both nationally and internationally. The perpetrators of cybercrime have not been fully prosecuted due to the weakness of the cyber legislation system in Indonesia and the limited number of experts available to handle this case. The perpetrators of cybercrime come from various countries, limited human resources and infrastructure are the main obstacles. It requires a strong commitment from the leadership, law enforcement institutions to improve the quality and quantity of human resources as well as preparation of an adequate budget for the procurement of facilities and infrastructure as well as establishing cooperation with higher education to accelerate the handling of existing limitations.[8]
b. Research by I Gusti Ayu Suanti Karnadi Singgi, I Gusti Bagus Suryawan, and I Nyoman Gede Sugiartha entitled "Law Enforcement Against Hacking as a Form of Cyber Crime", Journal of Legal Construction, Vol. 1 No. 2, October 2020. This study describes how law enforcement deals with criminal acts of hacking and how efforts are made to deal with cybercrime. Efforts to deal with mayantara crime or cybercrime have referred to the Information and Electronic Transaction Law, and various other efforts such as preventive efforts such as blocking, public education, and other positive things that can prevent a crime from occurring, as well as making repressive efforts. which efforts are made after the occurrence of a crime,[9]

[7] http://www.definition-pengertian.com/2015/05/pengertian-ruang-lingkup-kebijakan- Hukum.html, accessed on 09 July 2022, at 08:39 WIB
[8]Research by Yuwono Prianto, Nabila Annisa Fuzian, and Afif Farhan, "Constraints of Law Enforcement Against Cyber Crime During the Covid-19 Pandemic", Journal of Senapenmas, October 2021.
[9]I Gusti Ayu Suanti Karnadi Singgi, I Gusti Bagus Suryawan, and I Nyoman Gede Sugiartha entitled "Law Enforcement Against Hacking Crimes as a Form of Mayantara Crime (Cyber Crime)", Journal of Legal Construction, Vol. 1 No. 2, October 2020.

c. Research by Harjinder Singh Lallie, Lynsay A. Shepherd, Jason RC Nurse entitled "Cyber Security In The Age Of COVID-19: A Timeline And Analysis Of Cyber-Crime And Cyber-Attacks During The Pandemic", Elsevier Journal, Vol. 105, June 2021. This research analyzes the COVID-19 pandemic from a cybercrime perspective and sheds light on the various cyberattacks experienced globally during the pandemic. Cyberattacks are analyzed and considered in the context of major global events to uncover the modus operandi of cyberattack campaigns. The analysis shows how after what appeared to be a large gap between the initial outbreak of the pandemic in China and the first COVID-19 related cyber-attacks, attacks continued to become much more common until at some point in the day, three or four unique cyber-attacks were being reported.[10]

Articles written by this author have differences with the articles or studies above. The article written by this author discusses the growing mayantara crime in Indonesia and the government's efforts in enforcing the law against mayantara crime.

Research Methods

The researcher uses a normative juridical approach that is using a positivist legal idea. This concept oversees the law as a normative system that is independent, closed and detached from the real life of society.[11]The specification of the research used by the author is descriptive analysis, namely this research analysis does not go beyond the scope of variables, is deductive in nature, originates from general theories or concepts to explain a set of data with another set of data.[12]The sources and types of data used in this journal are secondary data which includes primary legal sources, secondary legal sources, and tertiary legal sources. The data collection technique used in this journal is document study or library sources, so this kind of data collection activity is called document study or library sources. The data analysis method used in this journal uses qualitative data analysis, namely analyzing and processing collected data in a systematic, orderly and structured manner.[13]

Results and Discussion

1. Law Enforcement as an Effort to Combat Cyber Crime

The development of information technology in the era of globalization which is growing and accompanied by the formation of information technology laws today should be followed by anticipatory steps by law enforcement officials to achieve balance and social order in the midst of group life, class, race and ethnicity, and society. , within a country or in relations with associations in the regional and international areas so as to create good protection and welfare for the Indonesian people as mandated by the fourth paragraph of the 1945 Constitution as the national goal of the Indonesian nation as well as a basic element of implementing a rule of law in Indonesia.

Law enforcement against cyber crimes is heavily influenced by legal factors. Because cyber crime is in the anatomy of transnational crime, the law used is national law, which in this discussion is Indonesian law. However, insofar as it is not regulated in national law, the principles, principles and rules of international law are used.

[10]Harjinder Singh Lallie, Lynsay A. Shepherd, Jason RC Nurse entitled "Cyber Security In The Age Of COVID-19: A Timeline And Analysis Of Cyber-Crime And Cyber-Attacks During The Pandemic", Elsevier Journal, Vol. 105, June 2021.
[11]Ibrahim, 2006, Theory and Methodology of Normative Law Research, Bayumedia Publishing, Malang.
[12]Soemanto, 2009, Technical Guidelines for Thesis Writing, Bumi Aksara, Jakarta, p.11
[13]Suteki and Taufani, 2020, Legal Research Methodology (Philosophy, Theory and Practice), Raja Grafindo Persada, Jakarta.

The prevention of cyber crime by law enforcement officials is strongly influenced by the existence of laws and regulations, there are several laws relating to information technology, especially crimes related to the internet before the enactment of the ITE Law. Cybercrime law enforcement prior to the enactment of the ITE Law was carried out by interpreting cybercrime into the Criminal Code legislation and specifically laws related to the development of information technology.

Recent developments, in order to regulate cyberspace and cyber crimes, Law Number 11 of 2008 concerning Information and Electronic Transactions has been issued as amended by Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 About Information and Electronic Transactions as a legal umbrella. It is hoped that the ITE Law will act as a controlling and law enforcement force for activities that use information technology not only limited to internet activities, but all activities that utilize computers and other electronic instruments.

This law has complied with the requirements of law enforcement both juridically, sociologically and philosophically. Philosophically, the enactment of Law Number 11 of 2008 concerning Information and Electronic Transactions as amended by Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Information and Electronic Transactions is based on the mandate contained in Article 28F of the Law -The 1945 Constitution of the Republic of Indonesia which states that every person has the right to communicate and obtain information properly to develop his personality and social environment, and has the right to seek, obtain, possess, store, process and convey information using all types of available channels . Juridically,

Sociologically, the public really needs Law Number 11 of 2008 concerning Information and Electronic Transactions as amended by Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Information and Electronic Transactions to regulate the various activities they carry out. do while interacting in cyberspace. The dynamics of globalization of information have demanded the existence of a rule to protect the interests of netters in accessing various information. The provisions in Law Number 11 of 2008 concerning Information and Electronic Transactions as amended by Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Information and Electronic Transactions are in line with religion, values and moral principles that are universally accepted so that the existence of cyber law (including international legal instruments that regulate it) is recognized, accepted and implemented by the information society. In the practice of law enforcement against any form of transnational crime, one of which is cybercrime, the main legal factor that often becomes an obstacle to law enforcement in practice is a matter of jurisdiction. The problem of doubts about the determination of jurisdiction in cyber space is actually acknowledged by the legal experts themselves. Tien S. Saefullah who stated that the jurisdiction of a country which is recognized by international law in the conventional sense, is based on geographical and time boundaries while communication and multimedia information are international in nature,[14]

Determining jurisdiction is a very important discourse in the framework of cyber law enforcement, especially in the context of law enforcement against transnational crimes. Issues regarding jurisdiction are regulated in Article 2 of Law Number 11 of 2008 concerning Information and Electronic Transactions as amended by Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Information and Electronic Transactions mentions this Law applies to everyone who takes legal actions as regulated in this Law, both within the jurisdiction of Indonesia and outside the jurisdiction of Indonesia, which has legal consequences in the jurisdiction of Indonesia and/or outside the jurisdiction of Indonesia and harms Indonesia's interests. Furthermore,

[14]Dikdik M. Arief Mansur and Elisatris Gultom, 2005, Cyber Law Legal Aspects of Information Technology, Refika Aditama, Bandung, p.34

The determination of the jurisdiction of cyber crimes can be studied from the principles of international law. There are two views from the state, namely that criminal law legislation applies to all criminal acts that occur within the territory of the state, whether committed by its own citizens or by foreigners (territorial principle). Second, criminal law legislation applies to all criminal acts committed by citizens, anywhere, even outside the territory of the state (personal principle). Also called the principle of active nationality. He further said that another reasonable basis for criminal law outside the state is the principle of protecting interests. It can be distinguished between protecting national interests (passive national principle) and protecting international interests (universal principle).[15]

According to Barda Nawawi Arief, discussing the issue of cyber jurisdiction is essentially related to issues of power or authority, namely who is in charge or who has the authority to regulate the internet world. Referring to the opinions of David R. Jhonson and Davis G. Post, Barda Nawawi Arief wrote about four competing models, namely:[16]

a. Execution of control exercised by the existing court bodies (the existing judicial forums).
b. National authorities carry out international agreements regarding the governance of cyber space.
c. Establishment of a new international organization (a New International Organization) that specifically deals with problems in the internet world. d. Government or self-governance by internet users.

One of the driving elements of legal substance is the legal structure. In order for the law to be beneficial, it requires the services of legal actors who are creative in translating the law in terms of the social interests that it must serve.[17]The legal structure intended to translate the law is law enforcement. Law enforcers or people in charge of enforcing the law cover a very broad scope. This is because it concerns officers at the upper, middle and lower strata. This means that in carrying out the task of implementing the law, officers should have a guideline, one of which is certain written regulations that cover the scope of their duties.[18]

Law enforcement includes components of the criminal justice system consisting of Police, Prosecutors, Judges, Advocates and Correctional Institutions. In law enforcement, H. Zainuddin Ali estimates the possibilities that law enforcement officers may face in carrying out law enforcement duties:[19]

a. To what extent officers are bound by existing regulations.
b. To what extent are officials willing to provide policies.
c. What kind of example should officials give to the community?
d. To what extent is the degree of synchronization of assignments given to officers so as to provide proper limits to their authority.

Based on the estimation presented by H. Zainuddin Ali, it can be analyzed the obstacles faced by law enforcers in tackling these cyber crimes. Law enforcers in enforcing the law often still use provisions in the Criminal Code even though there is already Law Number 11 of 2008 concerning Information and Electronic Transactions as amended by Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Information and Electronic Transactions (in the case of carding). This made the defendant easily escape the law because the elements of the article charged could not be proven.

[15]Moeljatno, 2000, Principles of Criminal Law, Bina Literacy, Jakarta, p. 38-40
[16]Barda Nawawi Arief, 2006, Mayantara's Crime (Development of Cybercrime Studies in Indonesia), Raja Grafindo Persada, Jakarta, pp. 29-30
[17]Bernard L. Tanya, Yoan N. Simanjuntak and Markus Yage, 2010, Legal Theory of Orderly Human Strategy across Space and Generations, Genta Publishing, Yogyakarta, p.213
[18]H. Zainuddin Ali, 2010, Legal Philosophy, Sinar Graphic, Jakarta, p.9
[19]Ibid, p.95

One indicator of legal compliance is the example set by law enforcers to the public. However, law enforcers often commit acts that are far from exemplary. It is rather difficult for law enforcers to take action against the perpetrators of cyber crimes while they themselves are actually the perpetrators or even the party protecting these cyber crimes. Under these conditions it is impossible to enforce legal consistency. The sophistication of technological developments apart from providing benefits for the welfare of society, has also been proven to be a precondition for increasing the modus operandi of crimes that develop in society. In reality, in a practical sense, it is often the case that the pace of technological growth that increases the sophistication of the modus operandi of crimes cannot be adequately followed by the police.[20]Not all police in the area have a cyber unit even though this crime is growing so widely.

Law enforcers in Indonesia are experiencing difficulties in dealing with the outbreak of cyber crimes. This is motivated by the fact that at least law enforcement officials understand the ins and outs of information technology (internet), besides that law enforcement officials in the regions are not ready to anticipate the rise of this crime because there are still many law enforcement officers who are technologically illiterate. there are still many law enforcement institutions in the regions that are not yet supported by an internet network.

2. Efforts to Handling the Occurrence of the Mayantara Crime

Law enforcement against cyber crimes is not yet optimal due to inadequate law enforcement facilities and infrastructure. Law enforcement against cyber crimes absolutely requires tools because the characteristics of these crimes are that they are committed with both tangible and intangible tools. Determination of the time and place of occurrence of cybercrimes is determined when the tool works effectively, therefore telematics analysis is needed in uncovering this crime. To investigate, detect and tackle this crime, Onno W. Purbo explained that the method really depends on the application and network topology used. Some of the applications are in gnacktrack and backtrack. This illustrates that adequate means and facilities are important in the law enforcement process. Without certain means or facilities, it is impossible for law enforcement to take place smoothly. These facilities or facilities include, among other things, educated and skilled human resources, good organization, adequate equipment, adequate finances, and so on. If these things are not fulfilled, it is impossible for law enforcement to achieve its goals.

Law No. 19 of 2016 which is an amendment to Law no. 11 of 2008 concerning Information and Electronic Transactions which is the largest legal instrument that is expected to accommodate all types of violations in the IT field. Besides having legal protection, there is also the threat of criminal sanctions for violations committed.

The government in making efforts to tackle mayantara crime on a national scale has implemented laws and regulations that specifically regulate IT. Law No. 19 of 2016 amendment to Law No.11 of 2008 concerning Information and Electronic Transactions. This borderless crime can be very dangerous if it is not addressed and does not have a strong legal framework to accommodate it.

Efforts to overcome these crimes can be in the form of preventive and repressive efforts:[21]

1. preventive efforts

This effort is a preventive effort made to prevent the emergence of a crime within the scope of society. Several things that can be done to prevent a crime from occurring are educating the public, blocking, and forming a National Cyber and Crypto Agency (BSSN).

[20]Romli Atmasasmita, 2007, Theory and Capita Selecta Criminology, Refika Aditama, Bandung, p.118
[21]I Gusti Ayu Suanti Karnadi Singgi, et al, Op. Cit, p. 338

2.repressive efforts

This effort is a conceptual effort, where this effort is carried out after the occurrence of a crime. This effort aims to take action against criminals such as imposing sanctions or imposing criminal sanctions according to the violations that have been committed.

The government needs to be more intensive in coordinating and partnering with religious leaders, community leaders and universities to find smooth solutions so that peace and balance can be maintained as well as at the same time preventing the escalation of the emotions of community groups which in turn can lead to actions However, the various legal principles contained in various laws and regulations and policy regulations must pay attention to the values that live in society. written so that all existing rules provide synergy with one another.It would be out of place if the legal principles contained in the ITE Law were clashed with other social norms.

Prevention and management of cyber crimes requires a penal and non-penal approach that is integral and requires integration. Talking about society is a necessity or obligation attached to discussions about law. Law and society are two sides of the same coin. So without discussing society first, actually talking about law is empty.[22]

Conclusion

Law enforcement in overcoming cyber crimes in Indonesia has not been implemented optimally. Factors that will affect law enforcement against cyber crimes include legal factors, law enforcement factors, facilities and facilities in law enforcement and community factors. Of these four factors, the factor that has the most influence on the weakness of existing law enforcement in dealing with cyber crimes in the anatomy of transnational crime is the legal factor (legal substance) which contains many weaknesses and law enforcement factors. The jurisdiction of cyber crimes is also very influential in law enforcement, considering the distance, cost and sovereignty of each country. Therefore international cooperation is needed either in mutual assistance, extradition agreements and agreements or cooperation with other countries related to cyber crimes or cyber crimes in law enforcement efforts in tackling information technology crimes. Efforts to overcome these crimes can be in the form of preventive efforts and repressive efforts. Preventive efforts are preventive efforts made to prevent the emergence of a crime within the scope of society. Repressive efforts are one of the efforts that are conceptual in nature, where these efforts are carried out after the occurrence of a crime. Preventive efforts are preventive efforts made to prevent the emergence of a crime within the scope of society. Repressive efforts are one of the efforts that are conceptual in nature, where these efforts are carried out after the occurrence of a crime. Preventive efforts are preventive efforts made to prevent the emergence of a crime within the scope of society. Repressive efforts are one of the efforts that are conceptual in nature, where these efforts are carried out after the occurrence of a crime.

References

Book

Achmad Ali, Revealing the Law (A Philosophical and Sociological Study), Publisher Toko Gunung Agung, Jakarta, 2002.

Barda Nawawi Arief, 2006, Mayantara's Crime (Development of Cybercrime Studies in Indonesia), Raja Grafindo Persada, Jakarta.

[22]Satjipto Rahardjo, 2009, Law and Good Life Behavior are Good Legal Basis, Kompas, Jakarta, p.9

Bernard L. Tanya, Yoan N. Simanjuntak and Markus Yage, 2010, Legal Theory of Orderly Human Strategy across Space and Generations, Genta Publishing, Yogyakarta.

Dikdik M. Arief Mansur and Elisatris Gultom, 2005, Cyber Law Legal Aspects of Information Technology, Refika Aditama, Bandung.

H. Zainuddin Ali, 2010, Legal Philosophy, Sinar Graphic, Jakarta.

Ibrahim, 2006, Theory and Methodology of Normative Law Research, Bayumedia Publishing, Malang.

Moeljatno, 2000, Principles of Criminal Law, Bina Literacy, Jakarta.

Romli Atmasasmita, 2007, Theory and Capita Selecta Criminology, Refika Aditama, Bandung.

Satjipto Rahardjo, 2009, Law and Good Life Behavior are Good Legal Basis, Kompas, Jakarta.

Soemanto, 2009, Technical Guidelines for Thesis Writing, Bumi Aksara, Jakarta.

Suteki and Taufani, 2020, Legal Research Methodology (Philosophy, Theory and Practice), Raja Grafindo Persada, Jakarta.

Journal Article

Budi Kristian Bivanda Putra, "Cyber Crime Application Policy in Indonesia", Pamulang Law Review, Vol.1 Issue 1, 2018.

Harjinder Singh Lallie, Lynsay A. Shepherd, Jason RC Nurse entitled “Cyber Security In The Age Of COVID-19: A Timeline And Analysis Of Cyber-Crime And Cyber-Attacks During The Pandemic”, Elsevier Journal, Vol. 105, June 2021.

I Gusti Ayu Suanti Karnadi Singgi, I Gusti Bagus Suryawan, and I Nyoman Gede Sugiartha entitled "Law Enforcement Against Hacking Crimes as a Form of Mayantara Crime (Cyber Crime)", Journal of Legal Construction, Vol. 1 No. 2, October 2020.

JPNN, 2020. Retrieved from the Number of Cyber Crimes Has Significantly Increased in the Last Five Years: https://www.jpnn.com/news/nomor-kejahatan-siber-menin_gkat-signifikan-dalam-lima-tahun-terakhir.

Ngafifi, "Technological Progress and Human Life Patterns in a Socio-Cultural Perspective", Journal of Educational Development: Foundations and Applications, Vol. 2 No.1, 2014.

Yuwono Prianto, Nabila Annisa Fuzian, and Afif Farhan, "Constraints of Law Enforcement Against Cyber Crime During the Covid-19 Pandemic", Senapenmas Journal, October 2021.

Copyrights